IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Criminal Action No.
	)	15-00339-01-CR-W-BP
CLARK H. HENSHAW,	)	
	)	
Defendant.	)	

REPORT AND RECOMMENDATION TO DENY DEFENDANT'S MOTION TO SUPPRESS

Before the Court is Defendant's Motion to Suppress Evidence. Defendant moves the Court to suppress evidence obtained from the August 26, 2013 search warrant issued to Google by the District of Maine and any subsequent warrants that relied on the fruits of that search. For the following reasons, Defendant's motion should be denied.

I. BACKGROUND

An indictment was returned on October 14, 2015, charging Defendant with one count of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2), one count of distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2), and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4). Defendant filed a motion to suppress (Doc. No. 20) and the government responded (Doc. No. 23). An evidentiary hearing was then held. The government appeared by Assistant United States Attorney Teresa Moore. Defendant was present, represented by appointed counsel Steve Moss. The government called Homeland Security Investigations Special Agent Anthony Castellanos and Homeland Security Investigations Special Agent Cassidy Casner to testify. The following exhibits were admitted into evidence:

Government's Exhibit 1: Application and Affidavit for Search Warrant; and
Government's Exhibit 2: Search Warrant.

II. EVIDENCE

On the basis of the evidence presented at the suppression hearing, I submit the following findings of fact.

1. Special Agent Anthohy Castellanos has been employed with Homeland Security Investigations since September of 2007, and is responsible for investigating child exploitation crimes (Tr. at 9).

2. In July of 2013, Special Agent Castellanos was assigned to work in Bangor, Maine (Tr. at 10). On July 25, 2013, he became involved in an investigation of an individual in Maine named "Patrick Ian Arsenault" for producing and distributing child pornography (Tr. at 10).

3. As part of this investigation, Special Agent Castellanos obtained a search warrant for Mr. Arsenault's residence for digital evidence and other items related to the production and distribution of child pornography (Tr. at 10). The search warrant was executed on August 21, 2013 (Tr. at 10). Digital evidence depicting Mr. Arsenault sexually abusing two minor children was recovered (Tr. at 10-11).

4. Mr. Arsenault told law enforcement during an interview that he had four primary trading partners and that he would receive child pornography in return for sending some out (Tr. at 11). Mr. Arsenault indicated that one of his primary trading partner's e-mail address included the word "Clark" (Tr. at 11). Mr. Arsenault traded child pornography using the e-mail account "jasonblodger@gmail.com" (Tr. at 21).

5. Forensic evaluation of an iPhone recovered during the search confirmed Mr.

Arsenault was trading child pornography with four primary trading partners, one of whom was "clarkumarkus@gmail.com" (Tr. at 11-12, 23, 24).

6. Based on the information recovered from Mr. Arsenault's residence and Mr. Arsenault's statement, Special Agent Castellanos applied for a search warrant under seal in the District of Maine for Google, which is located in the Northern District of California, to obtain information associated with the e-mail account for "clarkumarkus@gmail.com" (Tr. at 13, 14-15, 17, 27; Gvt. Exh. 1). Based on Mr. Arsenault's statement that he had been trading child pornography via e-mail for approximately one year, Special Agent Castellanos sought evidence related to the possession, distribution or production of child pornography from August 1, 2012 through August 26, 2013 (Tr. at 15, 16).

7. The search warrant application sought information associated with "clarkumarkus@gmail.com," including:

> **I. Information to be disclosed by Google**
>
> To the extent that the information described in Attachment A(1) is within the possession, custody, or control of Google, Google is required to disclose the following information to the government for each account or identifier listed in attachment A(1):
>
> a. The contents of all e-mails stored in the account (including copies of e-mails sent, draft e-mails and deleted e-mails from the account);
> b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
> c. All records or other information stored by an individual using the account, including address books, contacts, and photographs;
>
> **II. Information to be seized by the government**
>
> All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of the statutes listed in the warrant including, for each account or identifier listed on Attachment A(1),

information pertaining to the following matters:

a. Violations of Title 18 U.S.C. § 2251(a) (production of child pornography);
b. Violations of Title 19 U.S.C. §§ 2252(a)(4)(B) and 2252(a)(5)(B) (possession of child pornography);
c. Violations of Title 18 U.S.C. §§ 2252(a)(2) and 2252(a)(2) (distributing and receiving child pornography);
d. Records or information pertaining to an interest in child pornography; and
e. Records relating to who created, used, or communicated with the account or identifier.

(Gvt. Exh. 1, Attachment A-1 and B-1; Tr. at 24, 30).

8. Special Agent Castellanos testified that in applying for the search warrant for the "clarkumarkus" account, it would have been possible to only seek e-mail correspondence between "clarkumarkus" and "jasonblodger" from Google (Tr. at 26). Special Agent Castellanos did not know if Google would have fulfilled the request, though (Tr. at 26).

9. The warrant was authorized on August 26, 2013 (Tr. at 15; Gvt. Exh. 2).

10. The search warrant, including Attachments A-1 and B-1, was served on Google on August 26, 2013 via e-mail (Tr. at 16, 17). Special Agent Castellanos instructed Google not to disclose the issuance of the search warrant and to let him know if they had to notify the disclosure to the user (Tr. at 16, 27-28). Special Agent Castellanos did not notify "clarkumarkus" of the search warrant (Tr. at 17). There was not a court order preventing disclosure (Tr. at 28).

11. On August 30, 2013, Special Agent Castellanos obtained the results of the search warrant from Google (Tr. at 17; Gvt. Exh. 2). He performed a review of the contents, trying to confirm the trading of child pornography and determine the identity and location of the account user (Tr. at 31-32, 34). Special Agent Castellanos used a program that was designed to decipher e-mails by focusing on the issue of child pornography (Tr. at 32-33).

12. Special Agent Castellanos also issued an administrative subpoena on August 26,

2013, to T-Mobile seeking subscriber information for the phone number associated with "clarkumarkus" (Tr. at 13-14).

13. Special Agent Castellanos determined that the user associated with the "clarkumarkus" account was located in Lee's Summit, Missouri (Tr. at 18). The T-Mobile administrative subpoena revealed the subscriber of the phone number was Sean McGuire (Tr. at 18). A subpoena to Time Warner Cable revealed the IP address used to access the "clarkumarkus" account was an individual with the last name "McGuire" (Tr. at 18-19).

14. Based on this information, Special Agent Castellanos notified the Kansas City Homeland Security Investigations office of the lead and mailed them a disc containing the information pertaining to "clarkumarkus" obtained from the Google search warrant (Tr. at 19, 30-31).

15. Special Agent Cassidy Casner is assigned to Homeland Security Investigations in Kansas City (Tr. at 37). Special Agent Casner received the disc of information sent by Special Agent Castellanos (Tr. at 37-38). Special Agent Casner reviewed the contents of the disc and found it contained a large amount of e-mails containing child pornography (Tr. at 38-39).

16. The subscriber information revealed use of the Google drive, which is Google's cloud service (Tr. at 40). Special Agent Casner believed Defendant was primarily using a mobile device for Internet access, so she applied for another search warrant for "clarkumarkus@gmail.com" (Tr. at 40).

17. Special Agent Casner testified that had she not received the disc of information from Special Agent Castellanos, she would have applied for a search warrant herself based on the information obtained from Mr. Arsenault, the contents of Mr. Arsenault's e-mail account and the information related to the phone number that came back to Sean McGuire (Tr. at 40-41).

III. LEGAL ANALYSIS

Defendant seeks suppression of evidence that was seized pursuant to the August 26, 2013 search warrant executed on Google on grounds that (1) the District of Maine lacked jurisdiction to issue a warrant for evidence outside its district, (2) the warrant lacked the requisite particularity, and (3) law enforcement failed to notify Defendant of the search and seizure of data. Each argument will be addressed in turn.

A. JURISDICTION

Defendant first maintains that the court in Maine lacked jurisdiction to issue a warrant for evidence located in the Northern District of California. Defendant argues that the Stored Communications Act ("SCA") does not trump the limitations on a court's authority to issue warrants imposed by Federal Rule of Criminal Procedure 41(b) (providing a magistrate judge "has authority to issue a warrant to search for and seize a person or property located within the district") and 28 U.S.C. § 636 (noting territorial jurisdiction of the magistrate court).

Courts have repeatedly upheld courts' ability to issue warrants outside their respective district under the SCA. United States v. Berkos, 543 F.3d 392, 398 (7th Cir. 2008); United States v. Scully, 108 F. Supp. 3d 59, 83 (E.D. N.Y. 2015); Hubbard v. MySpace, Inc., 788 F. Supp. 2d 319, 325 (S.D. N.Y. 2011); United States v. Kernell, 2010 WL 1408437 at *4 (E.D. Tenn. Apr. 2, 2010); United States v. Freeman, 2010 WL 4386877 at * 12 n.6 (D. Minn. May 13, 2010); In re Search of Yahoo, 2007 WL 1539971 at *7 (D. Ariz. May 21, 2007); In re Search Warrant, 2005 WL 3844032 at *6 n.16 (M.D. Fla. Feb. 13, 2006). As explained in great depth by the Scully Court, this result is warranted by the plain language of both the SCA and Federal Rule of Criminal Procedure 41.

The SCA provides that a warrant for electronic communications may be issued "using the

procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction." 18 U.S.C. § 2703(a). A "court of competent jurisdiction" is defined as, inter alia, a court with "jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). This is not at odds with Federal Rule of Criminal Procedure 41. Although Rule 41(b) grants magistrates judges authority to "issue a warrant to search for and seize a person or property located within the district," subsection (a) of this same rule expressly provides that it "does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances." Section 2703 of the SCA is such a statue, as it regulates the search and seizure of electronic evidence.

Here, the magistrate judge in Maine had jurisdiction over the investigation of Ian Arsenault's distribution and receipt of child pornography and, thus, possessed the statutory authority to issue the warrant for Google in the Northern District of California. This result makes sense, as "[j]udicial and prosecutorial efficiency is better served by permitting the federal district court for the district where the crime allegedly occurred to preside over both the investigation and prosecution of that crime." See In re Search of Yahoo, 2007 WL 1539971 at *4 (citations omitted). Defendant's motion to suppress should be denied on this ground.

B. PARTICULARITY

Defendant next maintains that the warrant lacked the requisite particularity and, instead, amounted to a general warrant in violation of the Fourth Amendment. He specifically challenges "the search and seizure of all e-mails, records and other information associated with the 'clarkumarkus' account for a period of thirteen months."

"The Warrant Clause of the Fourth Amendment provides that 'no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly* describing the place

to be searched, and the persons or things to be seized.'" United States v. Sigillito, 759 F.3d 913, 923 (8th Cir. 2014)(emphasis in original). "Particularity prohibits the government from conducting 'general, exploratory rummaging of a person's belongings.'" Id. (citation omitted). "To satisfy the particularity requirement of the [F]ourth [A]mendment, the warrant must be sufficiently definite to enable the searching officers to identify the property authorized to be seized." Id. (citation omitted). "This particularity standard is one of 'practical accuracy rather than' of hypertechnicality." Id. (citation omitted). See also United States v. Summage, 481 F.3d 1075, 1079 (8th Cir. 2007). "Although '[t]he Fourth Amendment by its terms requires particularity in the warrant, not the supporting documents,' 'a court may construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant.'" United States v. Campbell, 764 F.3d 880, 887 (8th Cir. 2014). See also United States v. Hamilton, 591 F.3d 1017, 1024-25 (8th Cir. 2010). A warrant satisfies the particularity requirement when it authorizes search of property described in an attachment to the affidavit and the attachment describes the property to be searched in detail. Campbell, 764 F.3d at 887.

In United States v. Summage, the Eighth Circuit held that a warrant that authorized "the search and seizure of all video tapes and DVDs, pornographic pictures, video and digital recording devices and equipment, all equipment . . . used to develop, upload, or download photographs and movies, computers, and any indicia of occupancy" was sufficiently particular. 481 F.3d at 1079-80. The Court reasoned that because agents did not know "the nature of the format in which the sought-for video and photographs were created or stored, it was necessary to search a broad array of items for the relevant materials." Id.

In In the Matter of the Search of Information Associated with [redacted]@mac.com that

is Stored at Premises Controlled by Apple, Inc., the United States District Court for the District of Columbia specifically discussed particularity as it relates to e-mails. There, the government sought a search warrant applying to the e-mail account for "[redacted]@mac.com" that covered "information . . . dating from January 14, 2014, to the present, and stored at premises controlled by Apple Inc." 13 F. Supp. 3d 157, 161 (D. D.C. 2014). "Attachment B" to the application "set forth further details on the particular items to be seized," including:

> All e-mails, including e-mail content, attachments, source and destination addresses, and time and date information, that constitute evidence and instrumentalities of violations of 41 U.S.C. § 8702 . . . and 18 U.S.C. § 371 . . . , dated between January 14, 2014, to the present, including e-mails referring or relating to a government investigation involving any or all of the following: [individuals and entities have been redacted].

Id. In finding this language to satisfy the Fourth Amendment's particularity requirement, the Court noted that "the practical realities of searches for electronic records may require the government to examine information outside the scope of the search warrant to determine whether specific information is relevant to the criminal investigation and falls within the scope of the warrant." Id. at 166.

In In the Matter of the Search of Information Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corporation, the District of Kansas found that a search warrant application that contained very similar language[1] to the warrant at issue in this case

[1] The warrant application sought:

> The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, deleted emails, archived emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email, as well as the entirety of header information for each email;
>
> All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and

satisfied the particularity requirement. 2016 WL 5410401 at *9 (D. Kan. 2016). The Court discussed a collection of cases in which the search and seizure of entire e-mail accounts was permitted, stating limitations such as "a specified date range" or "referencing the violation of a specific criminal statute" helped prevent "the 'general rummaging' of [an] individual's e-mail account." Id. at *10. The Court concluded that "so long as a warrant specifies with

---

> source of payment (including any credit or bank account number);
>
> The types of service utilized and/or associated with this account to include all identifiers for these services and any connection logs associated with the usage of these services;
>
> All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
>
> All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

"Once the information was obtained from the Provider, the warrant application sought authorization for 'government-authorized persons' to review the records to seize items that:"

> Constitute fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy), 1029 (access device fraud), 1030 (computer intrusion), 1343 (wire fraud), and 2319 (copyright infringement), those violations involving [redacted], and others known and unknown, and occurring since September 7, 2008, including, for each account or identifier listed above, information pertaining to the following matters:
>
> a. Evidence of the scanning or theft of intellectual property to include copyright-protected material and those bearing trademarks;
> b. Evidence of using access drive(s) to fraudulently obtain intellectual property;
> c. Evidence of developing, using, or distributing tools or code to circumvent copy controls associated with intellectual property;
> d. Evidence of developing, using, or distributing software, code, or script as part of a "man-in-the-middle" computer intrusion;
> e. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
> f. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
> g. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);
> h. The identity of the person(s) who communicated with the user ID about matters relating to the scanning or theft of intellectual property, or the various means to steal the intellectual property such as access device fraud, computer intrusion, or circumventing copy controls, including records that help reveal their whereabouts.

2016 WL 5410401 at *1-*2.

particularity what evidence the Government intends to seize, establishes probable cause that the evidence is connected to a specific criminal statute, and includes some limitations (such as a date range) to prevent the potential of a general search, the warrant meets the Fourth Amendment particularity requirement." Id.

In this case, the warrant application identified with specificity the target account to be searched in Attachment A(1), that is information associated with "clarkumarkus@gmail.com." Attachment B(1) specifically described the information sought from Google (i.e., contents of all e-mails, all records or other information regarding the identification of the account, and all records or other information stored by an individual using the account to include address books, contacts and photographs), and connected the evidence to be seized by the government with specific criminal statues (i.e., 18 U.S.C. §§ 2251(a), 2252(a)(4)(B), 2252A(a)(5)(B), 2252(a)(2) and 2252A(A)(2)). Such information was limited to the time period from August 1, 2012 to August 26, 2013. I, therefore, find that the warrant was not lacking in particularity and recommend Defendant's motion to suppress be denied.

C. NOTIFICATION

Lastly, Defendant challenges the fact that he was not personally given notice of the search of his e-mail account. This argument is without merit. The Fourth Amendment does not require that the owner of an e-mail account be notified when a warrant is served upon the internet provider. In re United States, 665 F. Supp. 2d 1210, 1221-22, 1224 (D. Or. 2009) ("In this third party context, the Fourth Amendment notice requirement is satisfied when a valid warrant is obtained and served on the holder of the property to be seized, the [Internet service provider]."). See also Scully, 108 F. Supp. 3d at 83-84. Defendant's motion should be denied accordingly.

IV. CONCLUSION

For the above-stated reasons, it is

RECOMMENDED that the Court, after making an independent review of the record and the applicable law, enter an order denying Defendant's motion to suppress.

Counsel are advised that, pursuant to 28 U.S.C. § 636(b)(1), each has fourteen days from the date of this report and recommendation to file and serve specific objections to the same, unless an extension of time for good cause is obtained. Failure to file and serve timely specific objections may result in waiver of the right to appeal factual findings made in the report and recommendation which are accepted or adopted by the district judge except upon the ground of plain error or manifest injustice.

/s/ Robert E. Larsen
ROBERT E. LARSEN
United States Magistrate Judge

Kansas City, Missouri
February 23, 2017